PI 1171242

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office

May 18, 2004

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: *60/454,558*
FILING DATE: *March 14, 2003*
RELATED PCT APPLICATION NUMBER: *PCT/US04/07805*

By Authority of the
COMMISSIONER OF PATENTS AND TRADEMARKS

L. Edelen

L. EDELEN
Certifying Officer

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

03-17-03 60454558.01 Approved

PTO/SB/16 (10-01)
Approved for use through 10/31/2002. OMB 0651-0032
Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53 (c).

Express Mail Label No. EV 249512460 US

INVENTOR(S)		
Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
JUNBIAO	ZHANG	BRIDGEWATER, NJ.
SAURABH	MATHUR	PLAINSBORO, NJ

☐ *Additional inventors are being named on the _____ separately numbered sheets attached hereto*

TITLE OF THE INVENTION (500 characters max)

FLEXIBLE WLAN ACCESS POINT ARCHITECTURE CAPABLE OF ACCOMMODATING DIFFERENT USER DEVICE CAPABILITIES WITH STRONG SECURITY

CORRESPONDENCE ADDRESS

Direct all correspondence to:

☐ Customer Number
OR
Type Customer Number here

Place Customer Number Bar Code Label here

☒ Firm or Individual Name	JOSEPH S. TRIPOLI, THOMSON LICENSING INC.				
Address	PATENT OPERATIONS.				
Address	P. O. BOX 5312				
City	PRINCETON	State	NJ	ZIP	08543-5312
Country	USA	Telephone	609-734-6834	Fax	609-734-6888

ENCLOSED APPLICATION PARTS *(check all that apply)*

☒ Specification *Number of Pages* 4 ☐ CD(s), Number ☐

☐ Drawing(s) *Number of Sheets* ☐ ☐ Other (specify) ☐

☐ Application Data Sheet. See 37 CFR 1.76

METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT

☐ Applicant claims small entity status. See 37 CFR 1.27.

☐ A check or money order is enclosed to cover the filing fees

☒ The Commissioner is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number: 07-0832

☐ Payment by credit card. Form PTO-2038 is attached.

FILING FEE AMOUNT ($): 160

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

☒ No.

☐ Yes, the name of the U.S. Government agency and the Government contract number are: _____.

Respectfully submitted, SIGNATURE	Date: 3/14/03
TYPED or PRINTED NAME PAUL P. KIEL	REGISTRATION NO. 40,677 (*if appropriate*)
TELEPHONE 1 609 734 6815	Docket Number: PU030083

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, D.C., 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Box Provisional Application, Assistant Commissioner for Patents, Washington, D.C. 20231.

Express mail: EV 249512460 US

PU030083

FLEXIBLE WLAN ACCESS POINT ARCHITECTURE CAPABLE OF ACCOMMODATING DIFFERENT USER DEVICE CAPABILITIES WITH STRONG SECURITY

IEEE 802.11 based wireless LANs (WLANs) are becoming extremely popular these days. One particular problem facing WLANs is security, especially for WLANs deployed at public hot spots. How to provide secure access solutions that only allow authenticated accesses and protect authenticated user sessions from eavesdropping is the key problem to be solved in offering any public hot spot WLAN services. Compounding the problem is the fact that the users of the service may have wireless devices with different capabilities and configurations. In particular, some of these devices may be equipped with IEEE 802.1x client programs, while others may only have simple WEP based encryption mechanism. In this invention, we propose a wireless LAN access point solution that can accommodate such different user device capabilities and select the best available authentication mechanism for each wireless device accordingly. None of the existing WLAN access point or public hot spot access solution offers such a feature. We have built a prototype WLAN access point that integrated this feature and the solution has been tested and proven to work well.

As far as we know, none of the existing wireless LAN access points and public access solutions is capable of accommodating different types of wireless device capabilities.

Offering secure access at public WLAN hot spots has become increasingly important these days. There are several different ways in achieving such a goal in the existing solutions. The most promising solution uses IEEE 802.1x, which is becoming the standard in providing secure WLAN authentication. One problem with such a solution is that it requires IEEE 802.1x client software installation and configuration. Since, it was originally intended as an enterprise solution, many existing IEEE 802.1x clients are not convenient to use in public hot spots. In addition to these issues, the IEEE 802.1x protocol does not have a sophisticated mechanism for interacting with the user. The access point can only send simple one-way messages to the client via EAP notification. This may be sufficient for an enterprise setting but in a hot spot, the access point might want the user to accept an end user license before allowing access. Or, the access point might want to inform the user about the charges for the service. Our solution provides access point the capability to interact with the users via the web browser interface.

Another solution for secure access is based on the use of web browsers. It enables many user interactions and is very intuitive to the users. With certain enhancements such as those described in our earlier patent application [1], it can offer strong security. Thus we envision both approaches will co-exist and it is highly likely that a variety of wireless devices, with or without IEEE 802.1x capabilities, will be on the market for a long time. A public WLAN hot spot, therefore, should accommodate such different client capabilities, based on which the WLAN should select different authentication mechanisms. As far as we know, none of the existing public hot spot WLAN solutions has such a feature. In this disclosure, we describe our solution that can achieve this.

An embodiment architecture

The prototype that we have developed consists of the following key modules that are relevant to the current invention:

- 802.1X Engine

This module implements the IEEE 802.1X protocol with the enhancements that we propose. It is responsible for client detection and providing the client capability information to other modules of the system. In addition it also implements RADIUS client functionality to convert EAP messages to RADIUS messages.

- Packet Filter module

As the name suggests, the packet filter module is responsible for filtering packets based on the criteria set by other modules.

- HTTP server

Client detection

When a wireless client associates with the WLAN, the WLAN must first determine the client capability, i.e. whether it has an IEEE 802.1x client software. In order to understand how this can be done, we first look at the IEEE 802.1x protocol sequence in figure 1. As we can see from the figure, when the WLAN initiates the protocol sequence with a Request-Identity EAP packet, the IEEE 802.1x client always responds with a Response-Identity EAP packet. A wireless device without the IEEE 802.1x client will not be able to understand the Request-Identity EAP packet and thus won't send the right response. Based on this, the WLAN AP can detect wireless client capability and use the corresponding authentication mechanism for each client.

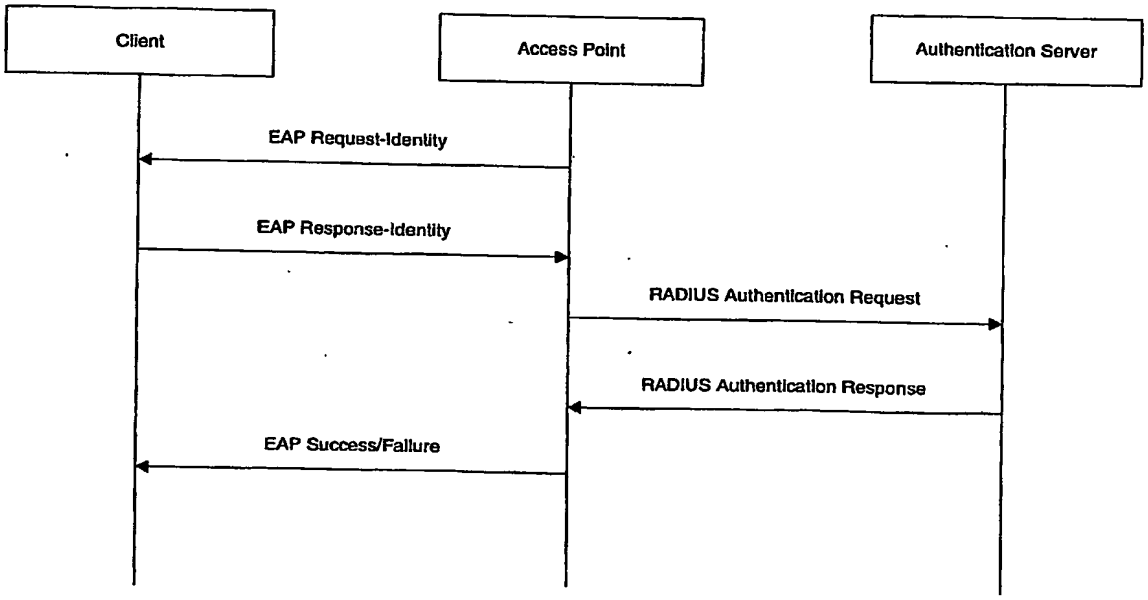

Figure 1. 802.1X Authentication Sequence

Authentication state management

Note that the client capability detection is done by the IEEE 802.1x engine at the AP. Such information must be conveyed to the higher layer to control client accesses. For example,

- for non IEEE 802.1x clients, IP packet filtering must be configured properly to redirect user HTTP requests to the local server, and when the HTTP requests are redirected, the HTTP server should present the users with information specifically related to the browser based authentication (see [1])

for IEEE 802.1x clients, besides allowing normal IEEE 802.1x protocol exchanges to go through, the AP also sets up proper IP packet filtering and state information for the HTTP server to control user accesses during and after IEEE 802.1x based authentication process.

As we can see from the above discussion, the WLAN system must maintain proper state information for the proper functioning of the system. Such state information will be supplied by the 802.1x engine and used by, among other things, the packet filtering function and the HTTP server. As an example embodiment, we shall describe how this is done in our prototype WLAN AP. The 802.1x engine may create one of the following states:

- 1x_progress: Indicates that the client is an IEEE 802.1x client and the 802.1x authentication process is ongoing.
- 1x_failure: Indicates that the 802.1x authentication process failed for some reason
- 1x_success: Indicates that the 802.1x authentication process succeeded
- non_1x: Indicates that the client is a non-IEEE 802.1x client. Because for such a client, all access controls are done at the higher layers, no further classification of state is necessary.

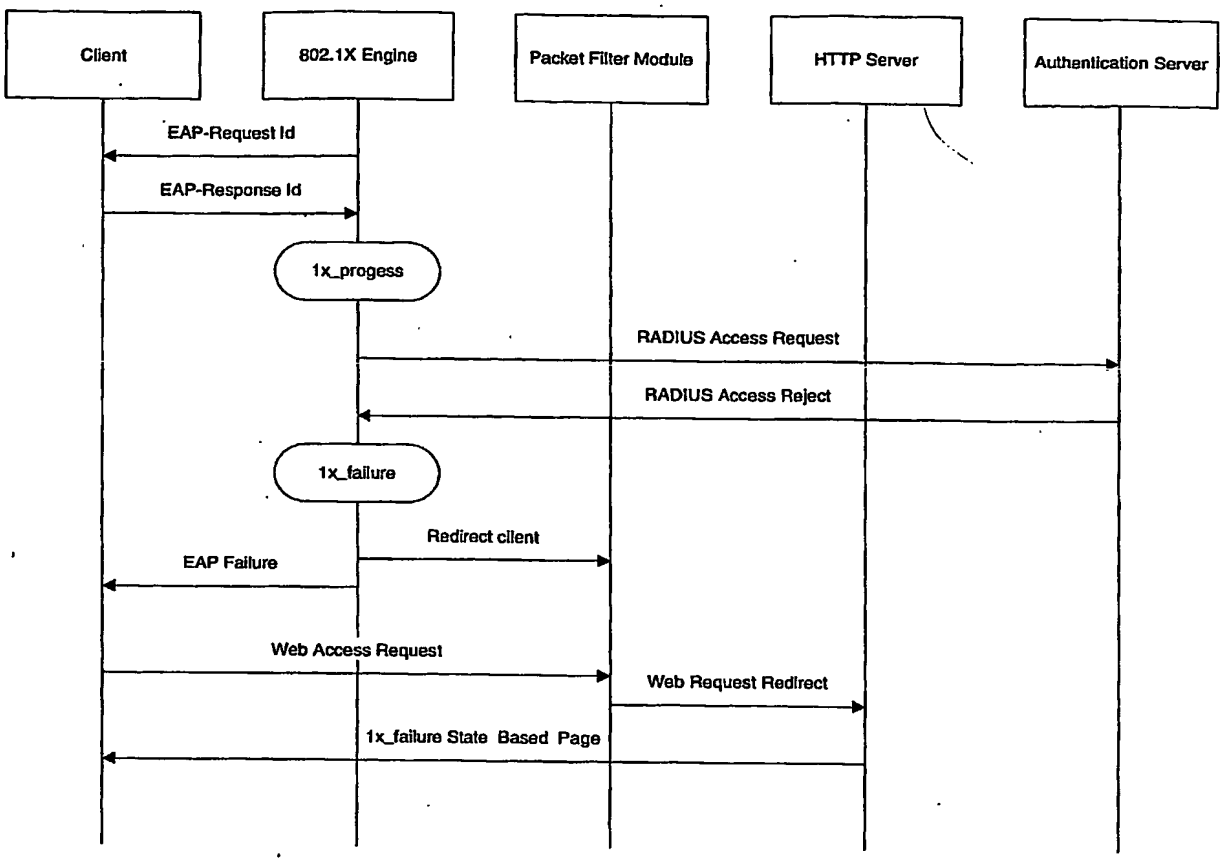

Figure 2. 802.1x authentication failure

As an example of how such information can be used, consider the case when an 802.1x client fails authentication for some reason (figure 2). When the client tries to access the web, the packet filtering function in the WLAN would redirect user requests to a local web page according to this state. The page may ask the user to check the 802.1x configuration, or try the web browser based authentication.

References:

[1] IU020369, Junbiao Zhang, Saurabh Mathur, Kumar Ramaswamy, "A WEB BROWSER BASED HOT SPOT WLAN ACCESS SOLUTION WITH STRONG SECURITYS"

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox